James E. Cecchi
CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700

[Additional Attorneys on Signature Page]

Attorneys for Plaintiffs and the proposed Classes

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

HASSAN SADRGILANY and DEBORAH DAMES, Individually and On Behalf of All Others Similarly Situated, Plaintiffs, v. T-MOBILE USA, INC., Defendant.	**Civil Action No.** CLASS ACTION COMPLAINT **JURY TRIAL DEMANDED**

Plaintiffs Hassan Sadrgilany and Deborah Dames ("Plaintiffs"), on behalf of themselves and others similarly situated, bring this class action against T-Mobile USA, Inc. ("T-Mobile" or the "Defendant"). Plaintiffs make the following allegations, except as to allegations specifically pertaining to Plaintiffs, upon information and belief based upon, *inter alia*, the investigation of counsel, and review of public documents.

NATURE OF THE ACTION

1. This is a class action on behalf of the over 53 million individuals whose sensitive personal identifying information was compromised in a cybersecurity breach of T-Mobile, which was announced on or about August 16, 2021 (the "T-Mobile Breach").

2. According to T-Mobile's public announcement of the T-Mobile Breach, the compromised information includes names, birth dates, Social Security numbers, driver's license numbers, phone numbers, and two types of identification numbers associated with mobile phones–IMEI and IMSI numbers.

3. T-Mobile failed to adequately protect consumers' sensitive personal identifying information. Lack of proper safeguards provided a means for unauthorized intruders to breach T-Mobile's computer network and steal sensitive personal identifying information.

4. Armed with this sensitive personal identifying information, hackers can commit a variety of crimes including, among other things, taking out loans in another person's name; opening new financial accounts in another person's name; using the victim's information to obtain government benefits; filing a fraudulent tax return and using the victim's information to obtain a tax refund; obtaining a driver's license or identification card in the victim's name but with another person's picture; or giving false information to police during an arrest.

5. As a result of the T-Mobile Breach, Plaintiffs and Class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class members must now and in the future closely monitor their financial accounts to guard against identity theft. Plaintiffs and Class members may be faced with fraudulently incurred debt. Plaintiffs and Class members may also incur out of pocket costs for, among other things, obtaining credit reports, credit freezes, or other protective measures to deter or detect identity theft.

6. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly-situated individuals and entities whose sensitive personal identifying information was accessed during the T-Mobile Breach.

7. Plaintiffs seek remedies including but not limited to reimbursement of out-of-pocket losses, further credit monitoring services with accompanying identity theft insurance, and improved data security.

PARTIES

8. Plaintiff Hassan Sadrgilany is a citizen of New Jersey who resides in Montvale, New Jersey.

9. Plaintiff Sadrgilany is a current T-Mobile customer. On or about August 20, 2021, he received a test message from T-Mobile notifying him that his personal information had been compromised.

10. Plaintiff Deborah Dames is a citizen of Missouri who resides in Chesterfield, Missouri.

11. Plaintiff Dames is a current T-Mobile customer. On or about August 19, 2021, she received a text message from T-Mobile notifying her that her personal information had been compromised.

12. Defendant T-Mobile USA, Inc. is incorporated in the state of Delaware with its principal place of business at 12920 SE 38th Street, Bellevue, Washington 98006. Defendant is a national telecommunications company that provides mobile communication services, among other products and services, throughout the United States and around the globe.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). If a class is certified in this action, the amount in controversy will exceed $5,000,000.00, exclusive of interest and costs. There are more than 100 members in the proposed class, and at least one member of the proposed class is a citizen of a state different from T-Mobile.

14. This Court has personal jurisdiction over Plaintiffs because Plaintiffs submit to the Court's jurisdiction.

15. This Court has personal jurisdiction over T-Mobile because it conducts business in the State of New Jersey, purposefully directs or directed its actions

toward New Jersey, and/or has the requisite minimum contacts with New Jersey necessary to permit the Court to exercise jurisdiction. This Court also has personal jurisdiction over T-Mobile because T-Mobile's conduct caused harm to Plaintiff Sadrgilany, as well as thousands of Class members residing in New Jersey.

16. Venue is also proper within this District because, pursuant to 28 U.S.C. § 1391(b)(2), a substantial part of the events or omissions giving rise to the claim occurred, or a substantial part of property that is the subject of the action is situated in this District. T-Mobile's conduct caused harm to Plaintiff Sadrgilany, as well as thousands of Class members residing in New Jersey.

SUBSTANTIVE ALLEGATIONS

THE T-MOBILE BREACH

17. On August 15, 2021, news media reported that hackers claimed to have stolen personal information for over 100 million individuals from T-Mobile. According to the hackers, the personal identifying information included customers' names, addresses, social security numbers, drivers' license information, phone numbers, dates of birth, security PINs, phone numbers, and, for some customers, unique IMSI and IMEI numbers (embedded in customer mobile devices that identify the device and the SIM card that ties that customer's device to a telephone number).

The hackers claimed to have doled the information into batches, some of which had already been sold and others that were, at the time, being marketed for sale.[1]

18. Reports indicate that a portion of the stolen T-Mobile customer data, including 30 million Social Security and driver's license numbers, was being marketed on the dark web for approximately $270,000.[2]

19. On August 16, 2021, T-Mobile released a statement confirming that "unauthorized access to some T-Mobile data had occurred," and that T-Mobile was continuing to investigate the data breach.[3]

20. On August 17, 2021, T-Mobile confirmed that the stolen data included "some personal information."[4]

21. On August 19, 2021, T-Mobile posted a "Notice of Data Breach" to its website, explaining that: "T-Mobile learned that a bad actor illegally accessed personal data. Our investigation is ongoing, but we have verified that a subset of T-

[1] *See, e.g.*, Lisa Vass, *100m T-Mobile Customer Records Purportedly Up for Sale*, Threatpost (Aug. 16, 2021 11:12 am), https://threatpost.com/t-mobile-investigates-100m-records/168689/; Joseph Cox, *T-Mobile Investigating Claims of Massive Customer Data Breach*, VICE (Aug. 15, 2021 11:03 am), https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million.

[2] *See* Joseph Cox, *supra* note 1.

[3] *T-Mobile Cybersecurity Incident Update*, T-Mobile (Aug. 16, 2021), https://www.t-mobile.com/news/network/cybersecurity-incident-update-august-2021.

[4] *T-Mobile Shares Additional Information Regarding Ongoing Investigation into Cyberattack*, T-Mobile (Aug. 17, 2021, Updated Aug. 20, 2021), https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation.

Mobile data had been accessed by unauthorized individuals and the data stolen from our systems did include some personal information."[5]

22. On August 20, 2021, T-Mobile posted a statement to its website confirming that:

a. "[A]pproximately 7.8 million current T-Mobile postpaid customer accounts that included first and last names, date of birth, [Social Security numbers], and driver's license/ID information was compromised[,]" in addition to phone numbers, IMEI, and IMSI information;

b. "5.3 million current postpaid customer accounts that had one or more customer names, addresses, dates of birth, phone numbers, IMEIs, and IMSIs illegally accessed";

c. "[D]ata files with information from about 40 million former or prospective T-Mobile customers, including first and last names, date of birth, [Social Security numbers], and driver's license/ID information were compromised";

[5] *Notice of Data Breach: Keeping you safe from cybersecurity threats*, T-Mobile (Aug. 19, 2021), https://www.t-mobile.com/brand/data-breach-2021.

d. "667,000 accounts of former T-Mobile customers . . . were accessed with customer names, phone numbers, addresses and dates of birth compromised";

e. "[A]pproximately 850,000 active T-Mobile prepaid customer names, phone numbers and account PINs were exposed."[6]

23. On information and belief, T-Mobile delayed directly notifying customers until on or after August 19, 2021.

24. Further, the T-Mobile Breach was not the first time Defendant was the subject of a cybersecurity breach. T-Mobile has been the target of many data breaches in the past, including at least four within the past three years.[7] As such, it knew that its systems were vulnerable and likely to be targeted by hackers seeking to obtain personal identifying information. Despite this knowledge, T-Mobile failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect its customers' personal information.

[6] *T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack*, *supra* note 4.

[7] Chris Velazco, *Here's what to do if you think you're affected by T-Mobile's big data breach*, Washington Post (Aug. 20, 2021 2:45 pm) https://www.washingtonpost.com/technology/2021/08/19/t-mobile-data-breach-what-to-do/.

25. In November 2019, hackers accessed personal identifying information for approximately one million T-Mobile prepaid customers, including names, phone numbers, account information, rates, and plan features.[8]

26. In March 2020, T-Mobile disclosed that it had experienced a data breach exposing customer and employee personal identifying information, including names, addresses, social security numbers, financial account information, government identification numbers, phone numbers and billing account information.[9]

27. In December 2020, T-Mobile discovered another data breach in which hackers accessed customer proprietary network information and undisclosed call-related information for hundreds of thousands of customers.[10]

---

[8] Devin Coldeway, *More than 1 million T-Mobile customers exposed by breach*, TechCrunch (Nov. 22, 2019 7:25 pm), https://techcrunch.com/2019/11/22/more-than-1-million-t-mobile-customers-exposed-by-breach/#:~:text=More%20than%201%20million%20T-Mobile%20customers%20exposed%20by,password%20data%29%20was%20exposed%20to%20a%20malicious%20actor.

[9] *T-Mobile Breach Leads to the Exposure of Employee Email Accounts and User Data*, Identity Theft Resource Center (Mar. 5, 2020), https://www.idtheftcenter.org/t-mobile-breach-leads-to-the-exposure-of-employee-email-accounts-and-user-data/#:~:text=On%20Thursday%2C%20March%204%2C%202020%2C%20T-Mobile%20disclosed%20a,separate%20data%20breach%20notification%20letters%20on%20their%20website.

[10] Alicia Hope, *Second Data Breach in 2020 for T-Mobile Exposed Customer and Call-Related Information of 200,000 Subscribers*, CPO Magazine (Jan. 11, 2021), https://www.cpomagazine.com/cyber-security/second-data-breach-in-2020-for-t-mobile-exposed-customer-and-call-related-information-of-200000-subscribers/#:~:text=T-Mobile%20suffered%20a%20data%20breach%20in%20which%20hackers,the%20fourth%20to%20hit%20the%20company%20since%202018.

28. In February 2021, T-Mobile notified customers that cyberthieves gained access to customer account information, including full names, addresses, email addresses, account numbers, Social Security numbers, account PINs, account security questions and answers, dates of birth, and plan information.[11]

29. Additionally, in 2017, a security researcher identified a vulnerability on a T-Mobile website that allowed hackers to access personal identifying information including email addresses, account numbers, and IMSI numbers.[12] That researcher explained

> T-Mobile has 76 million customers, and an attacker could have ran a script to scrape the data (email, name, billing account number, IMSI number, other numbers under the same account which are usually family members) from all 76 million of these customers to create a searchable database with accurate and up-to-date information of all users.[13]

According to a hacker, the bug had been exploited by multiple hackers over a multi-week period before it was discovered by the researcher, even uploading a video to YouTube demonstrating how to exploit the vulnerability.[14]

---

[11] Sergiu Gatlan, *T-Mobile discloses data breach after SIM swapping attacks*, Bleeping Computer (Feb. 26, 2021 3:18 pm), https://www.bleepingcomputer.com/news/security/t-mobile-discloses-data-breach-after-sim-swapping-attacks/.

[12] Lorenzo Franceschi-Bicchierai, *T-Mobile Website Allowed Hackers to Access Your Account Data With Just Your Phone Number*, Motherboard Tech (Oct. 10, 2017 2:03 pm), https://www.vice.com/en/article/wjx3e4/t-mobile-website-allowed-hackers-to-access-your-account-data-with-just-your-phone-number.

[13] *Id.*

[14] *Id.*

30. Despite these prior breaches, T-Mobile failed to adopt adequate protective measures to ensure that consumers' sensitive personal identifying information would not be improperly accessed.

31. Once T-Mobile's systems had been compromised, T-Mobile failed to timely discover the breach and implement adequate remedial measures to secure consumers' sensitive personal identifying information.

32. Moreover, T-Mobile failed to timely inform consumers of the T-Mobile Breach.

33. As a result of T-Mobile's inadequate measures, sensitive personal identifying information relating to over 53 million individuals was obtained from T-Mobile's computer network.

34. As a result of Defendant's failure to keep their personal identifying information from unauthorized access, Plaintiffs and Class members are in imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

35. Plaintiffs and Class members face a present and substantial risk of out-of-pocket fraud losses such as loans opened in their names, government benefits fraud, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

36. IMEI and IMSI numbers are identification numbers associated with a specific customer's phone. Because these numbers were included in the T-Mobile Breach, Plaintiffs and Class members are at risk for "SIM-swap attack[s]" which "could lead to account takeover concerns . . . since threat actors could gain access to two-factor authentication or one-time passwords tied to other accounts—such as email, banking, or any other account employing advanced authentication security feature—using a victim's phone number."[15]

37. Additionally, Plaintiffs and Class members face a present and substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their personal identifying information.

Plaintiff Hassan Sadrgilany

38. Plaintiff Hassan Sadrgilany is currently a T-Mobile customer and has been a T-Mobile customer since approximately 2013.

39. Since the announcement of the T-Mobile Breach, Plaintiff Sadrgilany has received an increased amount of spam and phishing emails and text messages.

40. On approximately August 20, 2021, Plaintiff Sadrgilany received a text message from T-Mobile alerting that "unauthorized access to some of [his] information, or others on your account, ha[d] occurred" and recommending that he

[15] Brian Barrett, *The T-Mobil Data Breach Is One You Can't Ignore*, Wired (Aug. 16, 2021 4:44 pm), https://www.wired.com/story/t-mobile-hack-data-phishing/.

"[l]earn more about practices that keep your account secure and general recommendations for protecting yourself[.]"

41. Since then, he has spent substantial time addressing the resulting privacy concerns, including researching the nature of the breach, and reviewing his financial and credit account statements for evidence of unauthorized activity, which he will continue to do for years into the future.

Plaintiff Deborah Dames

42. Plaintiff Deborah Dames is currently a T-Mobile customer and has been a T-Mobile customer since 2002.

43. On approximately August 19, 2021, Plaintiff Dames received a text message from T-Mobile alerting that "unauthorized access to some of [her] personal data ha[d] occurred" and recommending that she "take action to protect" her credit.

44. Since then, she has spent substantial time addressing the resulting privacy concerns, including researching the nature of the breach, and reviewing her financial and credit account statements for evidence of unauthorized activity, which she will continue to do for years into the future.

T-MOBILE'S POST-BREACH ACTIONS ARE INADEQUATE

45. In the wake of the T-Mobile Breach, Defendant has offered only inadequate services. T-Mobile is offering identify theft protection, Scam Shield (which includes call blocking and caller ID features), and "Account Takeover

Protection" services, Defendant places the burden on Plaintiffs and Class members by requiring them to expend the time to enroll in these services, instead of automatically enrolling all those impacted by the T-Mobile Breach.

46. Moreover, T-Mobile is only offering identity monitoring services for two years, even though the ramifications of personal identifying theft can extend far beyond two years.

47. T-Mobile has taken minimal steps to notify customers of the breach. Besides a terse text message sent to certain customers, T-Mobile has only posted statements to its website.

48. The Federal Communications Commission has opened an investigation into the T-Mobile Breach.[16]

CLASS ACTION ALLEGATIONS

49. Plaintiffs bring this class action pursuant to Fed. R. Civ. P. 23 on behalf of the following class and sub-classes:

> All individuals and entities in the United States whose personal identifying information was accessed in the cybersecurity breach announced by T-Mobile on August 16, 2021 (the "Nationwide Class"); and
>
> All individuals and entities in New Jersey whose personal identifying information was accessed in the cybersecurity

[16] Akanksha Rana, *T-Mobile breach hits 53 million customers as probe finds wider impact*, Reuters (Aug. 20, 2021 3:46 pm), https://www.reuters.com/technology/t-mobile-says-hackers-accessed-data-another-53-mln-subscribers-2021-08-20/.

> breach announced by T-Mobile on August 16, 2021 (the "New Jersey Sub-Class").
>
> All individuals and entities in Missouri whose personal identifying information was accessed in the cybersecurity breach announced by T-Mobile on August 16, 2021 (the "Missouri Sub-Class").

50. Excluded from the Nationwide Class, New Jersey Sub-Class, and Missouri Sub-Class are T-Mobile; any parent, subsidiary, or affiliate of T-Mobile or any employees, officers, or directors of T-Mobile; legal representatives, successors, or assigns of T-Mobile; and any justice, judge, or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer, as defined in 28 U.S.C. § 455(b).

51. Upon information and belief, the Nationwide Class, New Jersey Sub-Class, and Missouri Sub-Class consist of millions of geographically dispersed members, the joinder of whom in one action is impracticable. Disposition of the claims in a class action will provide substantial benefits to both the parties and the Court.

52. The rights of each member of the Nationwide Class, New Jersey Sub-Class, and Missouri Sub-Class were violated in a similar fashion based upon T-Mobile's uniform wrongful actions and/or inaction.

53. The following questions of law and fact are common to each Class member and predominate over questions that may affect individual Class members:

i. whether T-Mobile engaged in the wrongful conduct alleged herein;

ii. whether T-Mobile was negligent in collecting, storing, and/or safeguarding the sensitive personal identifying information of the Class members;

iii. whether T-Mobile owed a duty to Plaintiffs and Class members to adequately protect their personal information;

iv. whether T-Mobile breached its duties to protect the personal information of Plaintiffs and Class members;

v. whether T-Mobile knew or should have known that its data security systems and processes were vulnerable to attack;

vi. whether T-Mobile's conduct proximately caused damages to Plaintiffs and Class members;

vii. whether Plaintiffs and Class members are entitled to equitable relief including injunctive relief; and

viii. whether the Class members are entitled to compensation, monetary damages, and/or any other services or corrective measures from T-Mobile, and, if so, the nature and amount of any such relief.

54. Plaintiffs' claims are typical of the claims of the Nationwide Class, New Jersey Sub-Class, and Missouri Sub-Class in that Plaintiffs, like all Class members, had her sensitive personal identifying information compromised in the T-Mobile Breach.

55. Plaintiffs are committed to the vigorous prosecution of this action and will fairly and adequately represent and protect the interests of the proposed the Nationwide Class and Sub-Classes. Plaintiffs have no interests that are antagonistic to and/or that conflict with the interests of other putative Class members.

56. Plaintiffs have retained counsel competent and experienced in the prosecution of complex class action litigation.

57. The members of the proposed the Nationwide Class, New Jersey Sub-Class, and Missouri Sub-Class are readily ascertainable.

58. A class action is superior to all other available methods for the fair and efficient adjudication of the claims of the Nationwide Class, New Jersey Sub-Class, and Missouri Sub-Class. Plaintiffs and the Class members have suffered (and continue to suffer) irreparable harm as a result of T-Mobile's conduct. The damages suffered by some of the Class members may be relatively small, preventing those Class members from seeking redress on an individual basis for the wrongs alleged herein. Absent a class action, many Class members who suffered damages as a result of the cybersecurity breach of T-Mobile will not be adequately compensated.

59. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for T-Mobile. Additionally, adjudications with respect to individual Class members, such as adjudication as to injunctive relief, as a practical matter, would be dispositive of the interests of the other Class members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests.

COUNT ONE

NEGLIGENCE
(On behalf of the Nationwide Class and the New Jersey Sub-Class, and Missouri Sub-Class, in the Alternative)

60. Plaintiffs reallege and incorporate all allegations set forth in previous paragraphs as if fully set forth herein.

61. Upon coming into possession of the private, sensitive personal information of Plaintiffs' and the Class members, T-Mobile had (and continues to have) a duty to exercise reasonable care in safeguarding and protecting the information from being compromised and/or stolen. T-Mobile's duty arises from the common law, in part because it was reasonably foreseeable to T-Mobile that a breach of security was likely to occur under the circumstances and would cause damages to the Nationwide Class as alleged herein.

62. T-Mobile also had a duty to timely disclose to Plaintiffs and Class members that the T-Mobile Breach had occurred and that the sensitive personal identifying information of the Class members—particularly Social Security numbers, dates of birth, addresses, driver's license numbers—had been, or was reasonably believed to be, compromised. Such duty also arises under the common law because it was reasonably foreseeable to T-Mobile that a breach of security was likely to occur under the circumstances and would cause damages to the Nationwide Class as alleged herein.

63. T-Mobile, by and through its above negligent acts and/or omissions, further breached its duties to the Class members by failing to timely disclose to Plaintiffs and Class members that the T-Mobile Breach had occurred and that the sensitive personal identifying information of Plaintiffs and the Class members had been compromised.

64. T-Mobile also had a duty to put into place internal policies and procedures designed to detect and prevent the unauthorized dissemination of the Plaintiffs and Class members' sensitive personal identifying information. Such duty also arises under the common law because it was reasonably foreseeable to T-Mobile that a breach of security was likely to occur under the circumstances and would cause damages to the Nationwide Class as alleged herein.

65. T-Mobile, by and through its above negligent acts and/or omissions, unlawfully breach its duties to the Class members by, inter alia, failing to exercise reasonable care in protecting and safeguarding the Class members' sensitive personal identifying information within its possession, custody, and control.

66. But for T-Mobile's negligent and wrongful breach of the duties it owed (and continues to owe) to Plaintiffs and the Class members, the cybersecurity breach would not have occurred, and Plaintiffs' and the Class members' sensitive personal identifying information would never have been compromised.

67. The T-Mobile Breach and the above-described substantial injuries suffered by Plaintiffs and the Class members as a direct and proximate result of the breach were reasonably foreseeable consequences of T-Mobile's negligence.

COUNT TWO

NEGLIGENCE PER SE
(On behalf of the Nationwide Class and the New Jersey Sub-Class, and Missouri Sub-Class, in the Alternative)

68. Plaintiffs reallege and incorporate all allegations set forth in previous paragraphs as if fully set forth herein.

69. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice

of failing to use reasonable measures to protect sensitive personal identifying information.

70. In 2007, the FTC published guidelines which establish reasonable data security practices for businesses. The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vender-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

71. The FTC also has published a document entitled "Security Check: Reducing Risks to your Computer System" which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[17]

[17] *Security Check: Reducing Risks to Your Computer System*, FTC, https://www.ftc.gov/tips-advice/business-center/guidance/security-check-reducing-risks-your-computer-systems (last visited Aug. 25, 2021).

72. Further, the FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

73. By failing to have reasonable data security measures in place, T-Mobile engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

74. T-Mobile's violation of Section 5 of the FTC Act constitutes negligence *per se.*

75. Additionally, Missouri's Data Breach Notification Law, § 407.1500 of the Missouri Revised Statutes, requires anyone possessing personal information of residents of Missouri to "provide notice to the affected consumer that there has been a breach of security following discovery or notification of the breach . . . without reasonable delay. MO. Rev. Stat. § 407.1500.2(1) (West 2009).

76. The notice required by the Missouri Data Breach Notification Law must include a description of: "(a) [t]he incident in general terms; (b) [t]he type of personal information that was obtained as a result of the breach of security; (c) [a] telephone number that the affected consumer may call for further information and assistance, if one exists; (d) [c]ontact information for consumer reporting agencies; [and] (e) [a]dvice that directs the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports." MO. Rev. Stat. § 407.1500.4 (West 2009).

77. T-Mobile did not provide notice of the T-Mobile Breach to the Missouri Sub-Class that included the descriptions required under the Missouri Data Breach Notification Law. Specifically, T-Mobile's notice did not include a description of the incident, did not describe the personal information that had been breached, did not provide a telephone number for consumers to call for information and assistance, did not provide contact information for consumer reporting agencies, and did not advise recipients to review account statements and monitor credit reports.

78. Further, T-Mobile's text message notification to the Missouri Sub-Class was not made "without unreasonable delay." On information and belief, T-Mobile began notifying members of the Missouri Sub-Class of the T-Mobile Breach via text message on August 19, 2021, at least five days after the T-Mobile breach was known by the public and four days after T-Mobile publicly confirmed the breach.

79. T-Mobile's violation of Missouri's Data Breach Notification Law constitutes an independent basis of negligence *per se.*

80. Likewise, T-Mobile's violation of New Jersey's Consumer Security Breach Disclosure Act, N.J. Stat. Ann. §§ 56:8-163, *et seq.* constitutes an independent basis of negligence *per se*.

81. The T-Mobile Breach and the above-described substantial injuries suffered by Plaintiffs and the Class members as a direct and proximate result of the breach were reasonably foreseeable consequences of T-Mobile's negligence *per se*.

COUNT THREE

VIOLATION OF THE NEW JERSEY CONSUMER FRAUD ACT, N.J. Stat. Ann. § 56:8-1, *et seq.* (On behalf of the New Jersey Sub-Class)

82. Plaintiff Sadrgilany realleges and incorporates all allegations set forth in the previous paragraphs as if fully set forth herein.

83. T-Mobile, while operating in New Jersey, engaged, in unconscionable commercial practices, deception, misrepresentation, and the knowing concealment, suppression, and omission of material facts with intent that others rely on such concealment, suppression, and omission, in connection with the sale and advertisement of services, in violation of N.J. Stat. Ann. § 56:8-2. This includes, but is not limited to the following:

a. T-Mobile failed to enact adequate privacy and security measures to protect the sensitive personal identifying information of Plaintiff Sadrgilany and members of the New Jersey Sub-Class from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the T-Mobile Breach;

b. T-Mobile failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the T-Mobile Breach;

c. T-Mobile knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the sensitive personal identifying information of Plaintiff Sadrgilany and members of the New Jersey Sub-Class from unauthorized disclosure, release, data breaches, and theft;

d. T-Mobile omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for the sensitive personal identifying information from Plaintiff Sadrgilany and members of the New Jersey Sub-Class;

e. T-Mobile knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the sensitive personal identifying information of Plaintiff Sadrgilany and members of the New Jersey Sub-Class;

f. T-Mobile failed to maintain the privacy and security of the sensitive personal identifying information of Plaintiff Sadrgilany and New Jersey Sub-Class members, in violation of duties imposed by applicable

federal and state laws, directly and proximately causing the T-Mobile Breach; and

g. T-Mobile failed to disclose the T-Mobile Breach to Plaintiff Sadrgilany and the New Jersey Sub-Class members in a timely and accurate manner, in violation of the duties imposed by N.J. Stat. Ann. § 56:8-163(a).

84. As a direct and proximate result of T-Mobile's practices, Plaintiff Sadrgilany and the members of the New Jersey Sub-Class suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their sensitive personal identifying information of, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their the sensitive personal identifying information.

85. The above unlawful and deceptive acts and practices and acts by T-Mobile were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff Sadrgilany and the New Jersey Sub-Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

86. T-Mobile knew or should have known that its computer systems and data security practices were inadequate to safeguard the sensitive personal identifying information of Plaintiff Sadrgilany and New Jersey Sub-Class members and that the risk of a data breach or theft was highly likely. T-Mobile's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

87. Plaintiff Sadrgilany and the members of the New Jersey Sub-Class seek relief under N.J. Stat. Ann. § 56:8-19, including, but not limited to, injunctive relief, other equitable actual damages (to be proven at trial), treble damages, and attorneys' fees and costs.

COUNT FOUR

VIOLATION OF THE NEW JERSEY CONSUMER SECURITY BREACH DISCLOSURE ACT, N.J. Stat. Ann. § 56:8-163, *et seq.*
(On behalf of the New Jersey Sub-Class)

88. Plaintiff Sadrgilany realleges and incorporates all allegations set forth in the previous paragraphs as if fully set forth herein.

89. Under N.J. Stat. Ann. § 56:8-163(a), "[a]ny business that conducts business in New Jersey . . . that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is

reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay[.]"

90. T-Mobile is a business that conducts business in New Jersey that compiles or maintains computerized records that include personal information under N.J. Stat. Ann. § 56:8-163(a).

91. The sensitive personal identifying information of Plaintiff Sadrgilany and the members of the New Jersey Sub-Class that was compromised in the T-Mobile Breach includes personal information covered under N.J. Stat. Ann. §§ 56:8-163, *et seq*.

92. Because T-Mobile discovered a breach of its security system in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured, T-Mobile had an obligation to disclose the T-Mobile Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, *et seq*.

93. By failing to disclose the T-Mobile Breach in a timely and accurate manner, T-Mobile violated N.J. Stat. Ann. § 56:8-163(a).

94. As a direct and proximate result of T-Mobile's violations of N.J. Stat. Ann. § 56:8-163(a), Plaintiff Sadrgilany and the New Jersey Sub-Class members suffered the damages described above.

95. Plaintiff Sadrgilany and the New Jersey Sub-Class members seek relief under N.J. Stat. Ann. § 56:8-19, including but not limited to treble damages (to be proven at trial), attorneys' fees and costs, and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Nationwide Class, New Jersey Sub-Class, and Missouri Sub-Class, respectfully request that the Court certify this action as a class action, with Plaintiffs as class representatives and the undersigned counsel as class counsel, and enter an order of judgment against T-Mobile in favor of the Class that, *inter alia*:

A. awards actual damages to fully compensate the Nationwide Class, New Jersey Sub-Class, and Missouri Sub-Class for losses sustained as a direct, proximate, and/or producing cause of T-Mobile's unlawful conduct;

B. awards pre-judgment and post-judgment interest at the maximum allowable rates;

C. awards appropriate injunctive and equitable relief;

D. awards reasonable attorneys' fees and costs; and

E. orders any further relief that this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury to the extent permitted by law.

DATED: August 27, 2021

Respectfully submitted,

/s/ James E. Cecchi

James E. Cecchi
Kevin G. Cooper
CARELLA, BYRNE, CECCHI, OLSTEIN, BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700
jcecchi@carellabyrne.com
kcooper@carellabyrne.com

Joseph H. Meltzer
Melissa L. Troutner
KESSLER TOPAZ MELTZER & CHECK, LLP
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
jmeltzer@ktmc.com
mtrouther@ktmc.com

Christopher A. Seeger
Christopher L. Ayers
SEEGER WEISS LLP
55 Challenger Road, 6th Floor
Ridgefield Park, NJ 07660
Telephone: (973) 639-9100
Facsimile: (973) 679-8656
cseeger@seegerweiss.com
cayers@seegerweiss.com

Attorneys for Plaintiffs and the proposed Classes